UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Information associated with the Google LLC accounts, more fully described in Attachment A, that are stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered in Mountain View, California.	)	Case No. 21-1024M(NJ)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____
(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 12/28/2021 *(not to exceed 14 days)*

❒ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable Nancy Joseph .
(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____ .

Date and time issued: 12/14/2021 @ 4:21 p.m.

Nancy Joseph
Judge's signature

City and state: Milwaukee, Wisconsin

Honorable Nancy Joseph, U.S. Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information that is stored at premises owned, maintained, controlled, or operated by Google, Inc., an electronic service provider, headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043, and associated with the following account identifiers ("Target Accounts"):

- ibenready@gmail.com;
- Benready.br@gmail.com;
- Sssir454@gmail.com;
- Igetmoney.sjl79@gmail.com;
- lovenadiabanks@gmail.com;
- Msbenready.sl@gmail.com;
- purfektbih@gmail.com;

ATTACHMENT B

Information to be Seized

I. Information to be disclosed by Google LLC

To the extent the information described in Attachment A is within the possession, custody, or control of Google LLC, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Google LLC or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google LLC, is required to disclose the following information to the government for each user listed in Attachment A from January 1, 2012 to November 10, 2020:

1. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, and deleted emails; attachments; the source and destination addresses associated with each email; the size, length, and timestamp of each email; and true and accurate header information including the actual IP addresses of the sender and recipients of the emails;

2. All forwarding or fetching accounts relating to the accounts;

3. Any records pertaining to the user's contacts, including: address books; contact lists; social network links; groups, including Google Groups to which the user belongs or communicates with; user settings; and all associated logs and change history;

4. Any records pertaining to the user's calendar(s), including: Google Calendar events; Google Tasks; reminders; appointments; invites; and goals; the sender and recipients of any event invitation, reminder, appointment, or task; user settings; and all associated logs and change history;

5. The contents of all text, audio, and video messages associated with the account, including Chat, Duo, Hangouts, Meet, and Messages (including SMS, MMS, and RCS), in any format and however initially transmitted, including, but not limited to: stored, deleted, and draft messages, including attachments and links; the source and destination addresses associated with each communication, including IP addresses; the size, length, and timestamp of each communication; user settings; and all associated logs, including access logs and change history.

6. The contents of all records associated with the account in Google Drive (including Docs, Sheets, Forms, and Slides) and Google Keep, including: files, folders, media, notes and note titles, lists, and other data uploaded, created, stored, or shared with the account including drafts and deleted records; third-party application data and backups; SMS data

and device backups; the creation and change history of each record; accounts with access to or which previously accessed each record; any location, device, other Google service (such as Google Classroom or Google Group), or third-party application associated with each record; and all associated logs, including access logs and IP addresses, of each record;

7. The contents of all media associated with the account in Google Photos, including: photos, GIFs, videos, animations, collages, icons, or other data uploaded, created, stored, or shared with the account, including drafts and deleted records; accounts with access to or which previously accessed each record; any location, device, or third-party application data associated with each record; and all associated logs of each record, including the creation and change history, access logs, and IP addresses;

8. All maps data associated with the account, including Google Maps and Google Trips, including: all saved, starred, and privately labeled locations; search history; routes begun; routes completed; mode of transit used for directions; My Maps data; accounts and identifiers receiving or sending Location Sharing information to the account; changes and edits to public places; and all associated logs, including IP addresses, location data, and timestamps, and change history;

9. All Location History and Web & App Activity indicating the location at which the account was active, including the source of the data, date and time, latitude and longitude, estimated accuracy, device and platform, inferences drawn from sensor data (such as whether a user was at rest, walking, biking, or in a car), and associated logs and user settings, including Timeline access logs and change and deletion history;

10. All payment and transaction data associated with the account, such as Google Pay and Google Wallet, including: records of purchases, money transfers, and all other transactions; address books; stored credit; gift and loyalty cards; associated payment cards, including any credit card or bank account number, PIN, associated bank, and other numbers; and all associated access and transaction logs, including IP address, time stamp, location data, and change history; and

11. All Internet search and browsing history, and application usage history, including Web & App Activity, Voice & Audio History, Google Assistant, and Google Home, including: search queries and clicks, including transcribed or recorded voice queries and Google Assistant responses; browsing history, including application usage; bookmarks; passwords; autofill information; alerts, subscriptions, and other automated searches, including associated notifications and creation dates; user settings; and all associated logs and change history.

Google LLC is hereby ordered to disclose the above information to the government within 14 DAYS of service of this warrant.

II. Information to be seized by the government

All information described above in Section A that constitutes fruits, evidence, and instrumentalities of violations of Title 18, United States Code, Section 1591(a)(1) and (b)(2) (sex trafficking by force, fraud, or coercion) or Title 18, United States Code, Section 1594(b) (conspiracy to commit sex trafficking) involving Samuel L. Spencer and any co-conspirators, including:

1. Evidence related to posting of online commercial sex advertisements;

2. Images or videos of known or suspected sex trafficking victims, such as those taken for use in commercial sex advertisements or for communication with commercial sex buyers;

3. Communications with known or suspected sex trafficking victims or co-conspirators;

4. Messages, photographs, videos, memes, status updates, comments, or other postings;

5. Evidence of user attribution, showing who created or used the accounts at the time the things described in this warrant were created, edited, or deleted;

6. Evidence indicating how and when the accounts were accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the account owner(s) or user(s);

7. Evidence indicating the account owner(s) or user(s)'s state of mind as it relates to the crime under investigation; and

8. The identities of the person(s) who communicated with the accounts about matters relating to the above-listed offenses, including records that help reveal their whereabouts.

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information associated with the Google LLC accounts, more fully described in Attachment A, that are stored at premises owned, maintained, controlled, or operated by Google LLC., a company headquartered in Mountain View, California.

Case No. 21-1024M(NJ)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the _____ District of _____, there is now concealed *(identify the person or describe the property to be seized):*

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. Sections 1591(a)(1) and (b)(2) and 18 U.S.C. Section 1594(b)	Sex Trafficking by force, fraud and coercion and conspiracy

The application is based on these facts:

See Attached Affidavit

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Task Force Officer Heather Spranger, FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means).*

Date: 12/14/2021

Judge's signature

City and state: Milwaukee, Wisconsin

Honorable Nancy Joseph, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

I, HEATHER SPRANGER, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been employed with the Racine County Sheriff's Office since 2013 and am currently assigned the rank of Investigator. I am sworn and deputized as a Task Force Officer with the Federal Bureau of Investigation (FBI) and have been assigned to the FBI Milwaukee's Child Exploitation and Human Trafficking Task Force since December 2019. My duties include investigating violations of federal law, including but not limited to offenses involving the coercion, enticement, and sexual exploitation of minors, forced labor, and sex trafficking.

2. I am a law enforcement officer within the meaning of Title 18, United States Code, Section 2510(7), and I am empowered by law to conduct investigations, execute and serve search warrants, and make arrests for offenses enumerated in Title 18 of the United States Code or committed against the United States.

3. I have received training related to the investigation and enforcement of federal human trafficking laws. As a result of this training and my experience, I am familiar with the technologies traffickers use to recruit, communicate with, and exploit their victims. These include posting online advertisements for commercial sex dates, communicating electronically with prospective commercial sex buyers, and distributing sexually explicit images and videos of trafficking victims. I have also received more general training and gained experience in interviewing techniques, search warrant applications, the execution of searches and seizures, and the seizure, processing and identification of electronic evidence.

4. The facts in this affidavit come from my personal observations, my training and experience, information obtained from citizen witnesses, and information reported to me by other

law enforcement officers during the course of their official duties, all of whom I believe to be truthful and reliable.

PURPOSE OF AFFIDAVIT

5. I make this affidavit in support of applications for the following search warrants under Title 18, United States Code, Section 2703(c)(1)(A):

a. An application for a search warrant for information associated with certain Google accounts that is stored on computer servers at premises owned, maintained, controlled, or operated by **Google, LLC**. ("Google"), an electronic communications and remote computing service provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California. The "**Target Google Accounts**" are those accounts associated with the following email addresses:

a. ibenready@gmail.com;
b. benready.br@gmail.com;
c. sssir454@gmail.com;
d. igetmoney.sjl79@gmail.com;
e. lovenadiabanks@gmail.com;
f. msbenready.sl@gmail.com; and
g. purfektbih@gmail.com.

b. An application for a search warrant for information associated with certain Facebook user IDs that are stored at premises owned, maintained, controlled, or operated by **Facebook, Inc**. ("Facebook"), a social networking company headquartered in Menlo Park, California.

c. More specifically, I seek authorization to search Facebook's information associated with the following individual, whom I have identified by name as well as by Facebook account names (hereinafter the "**Target Facebook Accounts**"):

FACEBOOK ID (UID)	CURRENT DISPLAY NAME
Bengettingit.bengettingit	Bengettingit
Iben Gettingit	Iben.gettingit
Bena.fool.54	Bena Fool
Ben.afool.5	Ben Afool

Ben.readr	Ben Ready
100011387543641	Iben Ready

6. The information to be searched is described in the following paragraphs and in Attachment A to each application. The warrants I seek would require Google and Facebook to disclose to the government records and other information in their respective possessions pertaining to the subscribers or customers associated with the above-described identifiers, including the contents of communications. Upon receipt of the information described in Section I of Attachment B to each application, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

7. This affidavit is intended only to show that there is sufficient probable cause for the requested warrants. It does not set forth all of my knowledge about this matter.

JURISDICTION

8. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that SAMUEL L. SPENCER and others have committed violations of Title 18, United States Code, Sections 1591(a)(1) and (b)(2) (sex trafficking by force, fraud, or coercion) and Section 1594(b) (conspiracy to commit sex trafficking).

9. This Court has jurisdiction to issue the requested warrants because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) & 2703(c)(1)(A). Specifically, the Court is "a district court of the United States... that has jurisdiction over the offenses being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

10. Case agents have been investigating SAMUEL L. SPENCER for using force, fraud, and coercion to cause victims to engage in commercial sex acts during a period that spans from at least 2005 through 2020.

11. The investigation to date has revealed that SPENCER advertised most of his victims for commercial sex on websites such as, "Backpage.com," "Skipthegames.com," and "CityXGuide.com."

12. In my training and experience, I know that posting advertisements on these sites requires the creation of a user account that includes a linked email address. Some sites, such as Backpage.com, also require (or required, as Backpage is no longer operational) at least one linked form of payment. I also know that when a user posts and/or pays for an advertisement, a confirmation of that activity is typically automatically sent to that affiliated email account. If the ad cost money to post, the confirmation email will usually include the transaction amount, the form of payment used, and the name of the card or account holder.

13. The investigation has also revealed that many of SPENCER recruited, managed, controlled, and arranged sex dates for his victims using electronic messaging, including but not limited to SMS and MMS messaging, TextNow messaging, and social media direct messaging, including via **Facebook**.

14. There is probable cause to believe that the search warrants I seek for information from **Google** and **Facebook** will yield evidence of these activities.

A. Information Provided by Victim 1

15. On August 1, 2016, SPENCER was stopped for a traffic infraction by the Glendale Police Department. He had an active warrant for Battery from the Franklin Police Department and was arrested. The passenger of the vehicle SPENCER was driving was an adult female who will hereinafter be referred to as Victim 1. Victim 1 said she knew SPENCER as "Bin Laden." She disclosed to Glendale PD that SPENCER had been forcing her to engage in commercial sex acts since 2012 and taking all the profits of such activity.

16. Victim 1 told Glendale Police Department that she and SPENCER had met on **Facebook** and that SPENCER had reached out to her on that platform after she had been released from jail.

17. Victim 1 stated that SPENCER controlled when she ate, slept, and did prostitution dates. SPENCER was violent with Victim 1 at least once a week. SPENCER would physically assault Victim 1 when she did not do what SPENCER told her to do. Victim 1 expanded on these rules and punishments in several subsequent interviews between 2016 and the present, citing many specific examples.

18. Victim 1 stated that SPENCER would post advertisements for commercial sex acts featuring photographs of her. He paid for these ads using Paypal, Amazon gift cards, or Bitcoin.

19. Victim 1 said SPENCER used the name "BinReady" and various other combinations of "Bin Laden" and "Ready" in the email addresses he used for the accounts he created to post online advertisements for sex dates. Victim 1 further identified the email address **Ibenready@gmail.com** as an email associated with an account that Spencer used to post ads for sex dates online. She also recalled that one of SPENCER'S **Facebook** usernames was "**Iben Ready**."

20. For example, on April 24, 2017, an advertisement for sex dates was posted to Backpage.com (Post ID 17940134) entitled, "sweet juicing wet fun *come enjoy*." This advertisement featured photographs of Victim 1's face, as well as her body in various state of undress. The advertainment also featured photographs of Victim 2's body in various state of undress, as well as depicts her face, making it clearly identifiable as her. Subpoenaed records show that the advertisement was posted by the user account associated with **Ibenready@gmail.com**.

21. As another example, on April 27, 2019, an advertisement for sex dates was posted to Skipthegames.com with the tagline, "What you been looking for." This advertisement featured

three females in three separate photographs. Photograph 1 depicts a female further discussed below and referred to herein as Victim 3. Photograph 2 depicts Victim 1. She is identifiable in the photo by her tattoos, and she confirmed that SPENCER had taken the photo of her using his cell phone. The advertisement was posted by a user account associated with the email **sssir454@gmail.com**. According to Victim 1, it was SPENCER who posted the ad. Victim 1 stated that SPENCER used her photographs in various advertisements that featured multiple females that did sex dates for him.

22. During the course of this investigation, case agents served a search warrant on TextNow, a messaging application service, for several usernames including "sssir4544" and "sssir4545." The TextNow username "sssir4544" was established with the name "benready Sir." The TextNow username "sssir4545" was established using the name "Bengettingit Ready" and the email address **sssir454@gmail.com**. On November 2, 2020, the TextNow account "sssir4544" started using the signature "Benafool" at the end of messages. All of the mentioned usernames have been associated as name combinations associated with SPENCER, and SPENCER appears to have sent messages using that TextNow account (though it also appears that others used it at times). The messages in the account largely had to do with sex dates and drug trafficking.

23. Case agents located a commercial sex advertisement from Backpage.com (Post ID 18140769) posted April 21, 2017 and was entitled, "uPsCaLe RUssIAN and ITaliAN College BEauTY -21." The advertisement featured a female who went by the name "Nadia," which Victim 1 had identified as her working name. The advertisement featured photographs of Victim 1 that showed her face. This advertisement was posted by a user account associated with the email **lovenadiabanks@gmail.com.**

B. Information provided by Victim 2

24. SPENCER trafficked another adult female, hereinafter referred to as Victim 2, from approximately 2015 through 2017. Victim 2 was interviewed multiple times in 2021 about SPENCER. She explained that she first met him when she bought drugs from him in 2013. They met again in approximately December 2015 and became romantically involved. Almost immediately, Victim 2 moved into a trap house in Milwaukee with SPENCER and several other individuals. SPENCER persuaded Victim 2 that if she started doing prostitution dates for him, they could get a place of their own.

25. Within one week of moving in with SPENCER, Victim 2 began performing prostitution dates for him. SPENCER took sexually suggestive and explicit photos of Victim 2 and posted online ads for her as many as 6-8 times a day on websites including Backpage.com, Skip thegames.com, Intimate Encounters, LA69, Bedpage, Seeking Arrangement, and Ashley Madison. SPENCER also showed Victim 2 how to post ads.

26. Case agents have located some of these ads. For instance, on February 12, 2016, an ad was posted on Backpage.com (Post ID 14723473) for commercial sex dates that was entitled, "Hot, young and ready -21." The advertisement featured five photographs, four of which clearly depicted Victim 2's body and face, and one of which depicted just a buttock, but which Victim 2 said depicted her body. In one of the full-body photographs, in which Victim 2 is posing in lingerie, a black male can be seen in the reflection of a bathroom mirror. It appears the male is taking the photo, as he is holding up a cell phone, and there is a flash. Victim 2 viewed the photo and stated that the male was SPENCER and that she recognized the location to be a hotel room at the American Inn in Oak Creek, Wisconsin, where SPENCER frequently rented rooms for her to do prostitution dates. Victim 2 stated SPENCER took the photos for the purpose of creating prostitution ads, and he was the one who posted this advertisement online. Subpoenaed records

show that this advertisement was posted using the account associated with the email address **Ibenready@gmail.com**. Victim 2 identified that email as belonging to SPENCER.

27. Case agents also located commercial sex advertisements for Victim 2 on Skipthegames.com (Post IDs #779714828291 and #397665988935). The photographs on these ads featured Victim 2's face and therefore could be visually identified as her. The account used to post both advertisements was affiliated with email address **sssir454@gmail.com**.

28. SPENCER often beat Victim 2 if he felt that she was not doing sex dates fast enough, or not completing enough sex dates in a day. SPENCER beat Victim 2 multiple times while she was pregnant with his child. SPENCER told Victim 3 he wanted the pain from his beatings to last multiple days so she would remember what would happen if she disobeyed him again. Victim 2 once jumped out of SPENCER's car as they drove on the freeway to escape a beating.

C. Information provided by Victim 3

29. Yet another woman, hereinafter referred to as Victim 3, was trafficked by SPENCER between approximately 2014 and 2019. She has been interviewed multiple times in 2021 about SPENCER.

30. Victim 3 first met SPENCER when she bought drugs from him. Victim 3 knew SPENCER by the names "Sam," "Ben Ready," "Ben," "Ben Laden," "Bin Laden," and "Ibenready." Victim 3 stated the nickname "Ben" comes from SPENCER using the saying "I been ready" or "I stay ready." This means he is ready to make "moves" and "make money." Victim 3 described SPENCER as a "gorilla pimp" because he beat girls to make them "go out there" and make him money.

31. Roughly one week after meeting SPENCER, Victim 3 began performing sex dates and giving SPENCER all of her earnings in exchange for crack cocaine. Victim 3 was constantly

"indebted" to SPENCER for the drugs, and SPENCER put increasing pressure on her to do more prostitution dates for him.

32. Victim 3 described one instance where she said she was too tired to go out and do a sex date SPENCER was telling her to do. When Victim 3 told SPENCER, "No," he yelled at her, "Go make some money, Lazy Bitch!" SPENCER then beat Victim 3, bashing her head against a wooden floor, striking her in her head with a potted plant, and shoving dirt in her mouth. After the beating, SPENCER took Victim 3 to the date, however she was so badly beat up that the john turned Victim 3 away.

33. Victim 3 stated that there were advertisements for commercial sex dates featuring her posted on numerous websites such as Backpage.com and Skipthegames.com under the name "Jada." SPENCER posted the majority of the online ads for her, however Victim 3 posted some of the ads herself at SPENCER's direction. Victim 3 stated SPENCER used accounts associated with the email addresses **msbenready@gmail.com**, **benready.br@gmail.com**, and **Ibengettingit@gmail.com** to post advertisements for sex dates.

34. Case agents located several commercial sex ads for Victim 3. One such ad was posted on Backpage.com (Post ID 13661046) on November 14, 2015 and was entitled, "Come indulge with me in everything you've wanting……guaranteed satisfaction. -30." The ad featured a female listed as "Jada" and photographs of Victim 3 that showed her face. This ad was posted by a user account associated with the email address **benready.br@gmail.com**.

35. Case agents also located an ad from Backpage.com (Post ID 13920798) posted December 7, 2015 and entitled, "Meet Ms. Jada the Sexy Blonde you won't forget -36." The ad featured a female who went by the name "Jada." The ad featured a female listed as "Jada" and photographs of Victim 3 that showed her face. This ad was posted by a user account associated

with the email address **igetmoney.sjl79@gmail.com**, which I note uses Victim 3's initials and numbers associated with the year in which she was born.

36. Case agents located another commercial sex ad from Backpage.com (Post ID 13571877) posted November 6, 2015 and entitled, "Come indulge with me in everything you've wanting……guaranteed satisfaction. -30." The ad featured a female listed as "Jada" and photographs of Victim 3 that showed her face. This ad was posted by a user account associated with the email address **msbenready.sl@gmail.com**, a variation of the email identified by Victim 3 as belonging to SPENCER modified by adding her initials.

37. Between 2019 and 2020, a woman named Ericka Buie also posted ads for Victim 3. According to Victim 3, Buie acted as SPENCER's "bottom" during that time, posting ads for his victims, arranging dates for them, and arranging their transportation to and from sex dates. Buie did not do dates herself, however she had a "webcam business" in which she sold nude images and videos of herself.

38. Case agents identified an ad posted on Skipthegames.com (Post ID 398746030540) on March 28, 2020. It featured photos of Victim 1 (described above) and ten other females and was entitled, "BETTER THAN THE BEST 414-888-1568." The email associated with this advertisement is **purfektbih@gmail.com**. This email is similar to the name of Buie's website (Perfectbae.com) and Buie's Facebook username (Purfekt). The IP address associated with this advertisement was 75.10.183.46. AT&T records confirmed that Buie was the subscriber for that IP address. The return had a partial contact number for Buie, which was written as "414-888-XXXX." The digits displayed matched the number listed in the above ad of 414-888-1568. The billing address for the account was 2718 N 58th Street in Milwaukee, Wisconsin. Buie and SPENCER resided at that address during the time the above-mentioned advertisement was posted. (Law enforcement executed a search warrant there on November 10, 2020 and arrested SPENCER

at that address on other charges.) Skipthegames.com's records show that that IP address was used to post more than 300 commercial sex advertisements on their website from September 9, 2019 through August 23, 2020.

39. Victim 3 stated she often communicated with SPENCER on **Facebook Messenger**. They discussed sex dates, johns, drugs, and other illegal activities.

D. Facebook Accounts Located

40. A preservation request was submitted on December 6, 2021 to Facebook for the below-mentioned Facebook accounts to save information created starting in February 1, 2004 until December 7, 2021. Case agents located a large number of accounts belonging to SPENCER, including the accounts described herein.

41. **Bengettingit**: The profile pictures for this Facebook account are images of SPENCER. The account is "friends" on Facebook with accounts used by Victim 1 and Victim 3.

42. **Iben gettingit**: The profile pictures for this Facebook account are images of SPENCER. This Facebook account made "Facebook Wall" posts featuring Victims 1 and 2. Some of these posts (and others) referenced "pimping," "bitches" and "hoes," drug use, and derogatory remarks towards women. For instance, on August 10, 2017, **Iben gettingit** posted a photo of Victim 1 with the caption "When u home it's on." The following comments were observed below the post:

[Victim 2]: Back to getting pimped out and shooting up heroin together lol."

Iben gettingit: U would know.

[Victim 2]: So that's what you choose?

Iben gettingit: No u do

[Victim 2]: Who do you wanna be with??

Iben gettingit: U but u don't want me […]

43. **Bena Fool**: This Facebook account features a photograph of SPENCER'S child in common with Victim 2 as the "Profile Picture." It lists the user's date of birth as the same day and month as SPENCER's date of birth (March 5), though it lists a different year. The account is "friends" with an account used by Victim 1.

44. **Ben Afool**: The profile picture for this Facebook account features a photograph of SPENCER and Victim 2's child in common. There is another profile photograph that depicts SPENCER. This Facebook account features posts that depict large amounts cash and has "comments" on posts referring to a woman as a "ho."

45. **Ben Ready**: This Facebook account features a "Profile Picture" that depicts an image of SPENCER. It is Facebook "friends" with the **Ben Afool** account.

46. **Iben Ready**: As described above, this account was identified by Victims 1 and 3. This account has profile pictures that depict SPENCER, SPENCER with Victim 2, and cash. The **Iben** Ready account is "friends" with an account used by Victim 2, and there are publicly viewable photographs and "wall posts" featuring her on the page. The relationship status indicator on the **Iben Ready** account indicates that the user "married" Victim 2 on July 3, 2017. This Facebook account also commented on a Facebook post from an account used by Victim 3 with a photograph depicting Victim 3 with a large amount of cash.

TECHNICAL BACKGROUND

A. Background on Facebook

47. Facebook owns and operates a free-access social networking website of the same name that can be accessed at http://www.facebook.com. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

48. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birthdate, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers (for password retrieval), physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

49. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

50. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

51. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available

elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

52. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, the photos and videos associated with a user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

53. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e-mail messages, are sent to the recipient's "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a Chat feature that allows users to send and receive instant messages through Facebook. These chat communications are stored in the chat history for the account. Facebook also has a Video Calling feature, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

54. If a Facebook user does not want to interact with another user on Facebook, the first user can "block" the second user from seeing his or her account.

55. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages. Facebook users can "like" Facebook posts or updates, as well as webpages or content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become "fans" of particular Facebook pages.

56. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

57. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.

58. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs ("blogs"), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.

59. The Facebook Gifts feature allows users to send virtual "gifts" to their friends that appear as icons on the recipient's profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Facebook users can also send each other "pokes," which are free and simply result in a notification to the recipient that he or she has been "poked" by the sender.

60. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

61. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications ("apps") on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.

62. Some Facebook pages are affiliated with groups of users, rather than one individual user. Membership in the group is monitored and regulated by the administrator or head of the group, who can invite new members and reject or accept requests by users to enter. Facebook can identify all users who are currently registered to a particular group and can identify the administrator and/or creator of the group. Facebook uses the term "Group Contact Info" to describe the contact information for the group's creator and/or administrator, as well as a PDF of the current status of the group profile page.

63. Facebook uses the term "Neoprint" to describe an expanded view of a given user profile. The "Neoprint" for a given user can include the following information from the user's profile: profile contact information; news feed information; status updates; links to videos, photographs, articles, and other items; notes; wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications.

64. Facebook also retains Internet Protocol ("IP") logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile,

that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

65. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

66. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's "Neoprint," IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the

logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to "tag" their location in posts and Facebook "friends" to locate each other. This geographic and timeline information may tend to either inculpate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner's state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

67. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

B. BACKGROUND ON GOOGLE[1]

68. Google is a United States company that offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser called Google Chrome, a free search engine called Google Search, a free video streaming site

[1] The information in this section is based on information published by Google on its public websites, including, but not limited to, the following webpages: the "Google legal policy and products" page available to registered law enforcement at lers.google.com; product pages on support.google.com; or product pages on about.google.com.

called YouTube, a free mapping service called Google Maps, and a free traffic tracking service called Waze. Many of these free services offer additional functionality if the user signs into their Google Account.

69. In addition, Google offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Google also sells devices, including laptops, mobile phones, tablets, smart speakers, security cameras, and wireless routers. Users of Android and Google devices are prompted to connect their device to a Google Account when they first turn on the device, and a Google Account is required for certain functionalities on these devices.

70. Google advertises its services as "One Account. All of Google working for you." Once logged into a Google Account, a user can connect to Google's full suite of services offered to the general public, described in further detail below. In addition, Google keeps certain records indicating ownership and usage of the Google Account across services, described further after the description of services below.

71. When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information, including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

72. Signing up for a Google Account automatically generates an email address at the domain gmail.com. That email address will be the log-in username for access to the Google Account. Gmail can be accessed through a web browser or a mobile application. Additional email addresses ("recovery," "secondary," "forwarding," or "alternate" email addresses) can be associated with the Google Account by the user. Google preserves emails associated with a Google Account indefinitely, unless the user deletes them.

73. Google offers a map service called Google Maps which can be searched for addresses or points of interest. Google Maps can provide users with turn-by-turn directions from one location to another using a range of transportation options (driving, biking, walking, etc.) and real-time traffic updates. Users can share their real-time location with others through Google Maps by using the Location Sharing feature. And users can find and plan an itinerary using Google Trips. A Google Account is not required to use Google Maps, but if users log into their Google Account while using Google Maps, they can save locations to their account, keep a history of their Google Maps searches, and create personalized maps using Google My Maps. Google stores Maps data indefinitely, unless the user deletes it.

74. A subsidiary of Google, Google Payment Corporation, provides Google Accounts an online payment service called Google Pay (previously Google Wallet), which stores credit cards, bank accounts, and gift cards for users and allows them to send or receive payments for both online and brick-and-mortar purchases, including any purchases of Google services. Users may delete some data associated with Google Pay transactions from their profile, but Google Payment Corporation retains some records for regulatory purposes.

75. Google offers a cloud-based photo and video storage service called Google Photos. Users can share or receive photos and videos with others. Google Photos can be trained to recognize individuals, places, and objects in photos and videos and automatically tag them for easy retrieval via a search bar. Users have the option to sync their mobile phone or device photos to Google Photos. Google preserves files stored in Google Photos indefinitely, unless the user deletes them.

76. Google Drive is a cloud storage service automatically created for each Google Account. Users can store an unlimited number of documents created by Google productivity applications like Google Docs (Google's word processor), Google Sheets (Google's spreadsheet

program), Google Forms (Google's web form service), and Google Slides, (Google's presentation program). Users can also upload files to Google Drive, including photos, videos, PDFs, and text documents, until they hit the storage limit. Users can set up their personal computer or mobile phone to automatically back up files to their Google Drive Account. Each user gets 15 gigabytes of space for free on servers controlled by Google and may purchase more through a subscription plan called Google One. In addition, Google Drive allows users to share their stored files and documents with up to 100 people and grant those with access the ability to edit or comment. Google maintains a record of who made changes when to documents edited in Google productivity applications. Documents shared with a user are saved in their Google Drive in a folder called "Shared with me." Google preserves files stored in Google Drive indefinitely, unless the user deletes them.

77. Google provides an appointment book for Google Accounts through Google Calendar, which can be accessed through a browser or mobile application. Users can create events or RSVP to events created by others in Google Calendar. Google Calendar can be set to generate reminder emails or alarms about events or tasks, repeat events at specified intervals, track RSVPs, and auto-schedule appointments to complete periodic goals (like running three times a week). A single Google Account can set up multiple calendars. An entire calendar can be shared with other Google Accounts by the user or made public so anyone can access it. Users have the option to sync their mobile phone or device calendar so it is stored in Google Calendar. Google preserves appointments indefinitely, unless the user deletes them. Calendar can be accessed from the same browser window as other Google products like Gmail and Calendar.

78. Google provides an address book for Google Accounts through Google Contacts. Google Contacts stores contacts the user affirmatively adds to the address book, as well as contacts the user has interacted with in Google products. Google Contacts can store up to 25,000 contacts.

Users can send messages to more than one contact at a time by manually creating a group within Google Contacts or communicate with an email distribution list called a Google Group. Users have the option to sync their Android mobile phone or device address book with their account so it is stored in Google Contacts. Google preserves contacts indefinitely, unless the user deletes them. Contacts can be accessed from the same browser window as other Google products like Gmail and Calendar.

79. Google offers a free web browser service called Google Chrome which facilitates access to the Internet. Chrome retains a record of a user's browsing history and allows users to save favorite sites as bookmarks for easy access. If a user is logged into their Google Account on Chrome and has the appropriate settings enabled, their browsing history, bookmarks, and other browser settings may be saved to their Google Account in a record called My Activity. My Activity also collects and retains data about searches that users conduct within their own Google Account or using the Google Search service while logged into their Google Account, including voice queries made to the Google artificial intelligence-powered virtual assistant Google Assistant or commands made to Google Home products. Google also has the capacity to track the websites visited using its Google Chrome web browser service, applications used by Android users, ads clicked, and the use of Google applications by iPhone users. According to Google, this search, browsing, and application use history may be associated with a Google Account when the user is logged into their Google Account on the browser or device and certain global settings are enabled, such as Web & App Activity. Google Assistant and Google Home voice queries and commands may also be associated with the account if certain global settings are enabled, such as Voice & Audio Activity tracking. Google maintains these records indefinitely for accounts created before June 2020, unless the user deletes them or opts in to automatic deletion of their location history every three or eighteen months. Accounts created after June 2020 auto-delete Web & App Activity

after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.

80. Google provides several messaging services including Duo, Messages, Hangouts, Meet, and Chat. These services enable real-time text, voice, and/or video communications through browsers and mobile applications, and also allow users to send and receive text messages, videos, photos, locations, links, and contacts. Google may retain a user's messages if the user hasn't disabled that feature or deleted the messages, though other factors may also impact retention. Google does not retain Duo voice calls, though it may retain video or voicemail messages.

81. Google integrates its various services to make it easier for Google Accounts to access the full Google suite of services. For example, users accessing their Google Account through their browser can toggle between Google Services via a toolbar displayed on the top of most Google service pages, including Gmail and Drive. Google Hangout, Meet, and Chat conversations pop up within the same browser window as Gmail. Attachments in Gmail are displayed with a button that allows the user to save the attachment directly to Google Drive. If someone shares a document with a Google Account user in Google Docs, the contact information for that individual will be saved in the user's Google Contacts. Google Voice voicemail transcripts and missed call notifications can be sent to a user's Gmail account. And if a user logs into their Google Account on the Chrome browser, their subsequent Chrome browser and Google Search activity is associated with that Google Account, depending on user settings.

82. Google collects and retains data about the locations at which Google Account services are accessed from any mobile device, as well as the periodic location of Android devices while they are in use. This location data can derive from a range of sources, including GPS data, Wi-Fi access points, cell-site locations, geolocation of IP addresses, sensor data, user searches,

and Bluetooth beacons within range of the device. According to Google, this location data may be associated with the Google Account signed-in or registered to the device when Location Services are activated on the device and the user has enabled certain global settings for their Google Account, such as Location History or Web & App Activity tracking. The data retained may be both precision location data, like latitude and longitude coordinates derived from GPS, and inferential location data, such as the inference that a Google Account's user is in New York because the user conducts a series of searches about places to eat in New York and directions from one New York location to another. Precision location data is typically stored by Google in an account's Location History and is assigned a latitude-longitude coordinate with a meter radius margin of error. Inferential data is stored with an account's Web & App Activity. Google maintains these records indefinitely for accounts created before June 2020, unless the user deletes it or opts to automatically delete their Location History and Web & App Activity after three or eighteen months. Accounts created after June 2020 auto-delete Location History after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.

83. Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website or using a mobile application), details about the devices used to access the account, and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's terms of service, as well as the IP addresses associated with particular logins to the account. Because every device that connects

to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the Google Account.

84. Google maintains the communications, files, and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a communication or file from their Google Account, it may continue to be available on Google's servers for a certain period of time.

85. In my training and experience, evidence of who was using a Google account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. For example, a user's saved Maps locations, IP addresses, contacts, photos, and calendar appointments can all reveal the user's identity. Many of these features could also establish where the user was at relevant times, such as whether SPENCER was at a particular motel on a date when a victim was known to have been engaging in commercial sex dates there.

86. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Google can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time, may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account.

Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

87. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and internet searches/access are often used in furtherance of criminal activity, including to communicate about and facilitate sex trafficking, and there is probable cause to believe that SPENCER did so in this case, as described above. For instance, SPENCER used Gmail email addresses to receive notifications about the commercial sex ads he posted for his victims and took photos of his victims for use in the ads. He used the Internet, accessed through web browsing services, to post the ads. He used message and phone services to communicate with his victims, communicate with prospective johns on their behalf. Thus, stored communications and files connected to a Google Account may provide direct evidence of the offenses under investigation.

88. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (*e.g.,* information indicating a plan to commit a crime), or consciousness of guilt (*e.g.,* deleting account information in an effort to conceal evidence from law enforcement).

89. Other information connected to the use of a Google account may lead to the discovery of additional evidence. For example, the apps downloaded from the Google Play store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. These could include, for instance, apps SPENCER used to make and receive payments, such as PayPal or CashApp. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

90. Therefore, Google's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Google services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

CONCLUSION

91. Based on the foregoing, I request that the Court issue the proposed search warrants.

92. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. Because the government will execute this warrant by serving the warrants on Google and Facebook, who will compile the requested records at a time convenient to them, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A

Property to Be Searched

This warrant applies to information that is stored at premises owned, maintained, controlled, or operated by Google, Inc., an electronic service provider, headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043, and associated with the following account identifiers ("Target Accounts"):

- ibenready@gmail.com;
- Benready.br@gmail.com;
- Sssir454@gmail.com;
- Igetmoney.sjl79@gmail.com;
- lovenadiabanks@gmail.com;
- Msbenready.sl@gmail.com;
- purfektbih@gmail.com;

ATTACHMENT B

Information to be Seized

I. Information to be disclosed by Google LLC

To the extent the information described in Attachment A is within the possession, custody, or control of Google LLC, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Google LLC or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google LLC, is required to disclose the following information to the government for each user listed in Attachment A from January 1, 2012 to November 10, 2020:

1. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, and deleted emails; attachments; the source and destination addresses associated with each email; the size, length, and timestamp of each email; and true and accurate header information including the actual IP addresses of the sender and recipients of the emails;

2. All forwarding or fetching accounts relating to the accounts;

3. Any records pertaining to the user's contacts, including: address books; contact lists; social network links; groups, including Google Groups to which the user belongs or communicates with; user settings; and all associated logs and change history;

4. Any records pertaining to the user's calendar(s), including: Google Calendar events; Google Tasks; reminders; appointments; invites; and goals; the sender and recipients of any event invitation, reminder, appointment, or task; user settings; and all associated logs and change history;

5. The contents of all text, audio, and video messages associated with the account, including Chat, Duo, Hangouts, Meet, and Messages (including SMS, MMS, and RCS), in any format and however initially transmitted, including, but not limited to: stored, deleted, and draft messages, including attachments and links; the source and destination addresses associated with each communication, including IP addresses; the size, length, and timestamp of each communication; user settings; and all associated logs, including access logs and change history.

6. The contents of all records associated with the account in Google Drive (including Docs, Sheets, Forms, and Slides) and Google Keep, including: files, folders, media, notes and note titles, lists, and other data uploaded, created, stored, or shared with the account including drafts and deleted records; third-party application data and backups; SMS data

and device backups; the creation and change history of each record; accounts with access to or which previously accessed each record; any location, device, other Google service (such as Google Classroom or Google Group), or third-party application associated with each record; and all associated logs, including access logs and IP addresses, of each record;

7. The contents of all media associated with the account in Google Photos, including: photos, GIFs, videos, animations, collages, icons, or other data uploaded, created, stored, or shared with the account, including drafts and deleted records; accounts with access to or which previously accessed each record; any location, device, or third-party application data associated with each record; and all associated logs of each record, including the creation and change history, access logs, and IP addresses;

8. All maps data associated with the account, including Google Maps and Google Trips, including: all saved, starred, and privately labeled locations; search history; routes begun; routes completed; mode of transit used for directions; My Maps data; accounts and identifiers receiving or sending Location Sharing information to the account; changes and edits to public places; and all associated logs, including IP addresses, location data, and timestamps, and change history;

9. All Location History and Web & App Activity indicating the location at which the account was active, including the source of the data, date and time, latitude and longitude, estimated accuracy, device and platform, inferences drawn from sensor data (such as whether a user was at rest, walking, biking, or in a car), and associated logs and user settings, including Timeline access logs and change and deletion history;

10. All payment and transaction data associated with the account, such as Google Pay and Google Wallet, including: records of purchases, money transfers, and all other transactions; address books; stored credit; gift and loyalty cards; associated payment cards, including any credit card or bank account number, PIN, associated bank, and other numbers; and all associated access and transaction logs, including IP address, time stamp, location data, and change history; and

11. All Internet search and browsing history, and application usage history, including Web & App Activity, Voice & Audio History, Google Assistant, and Google Home, including: search queries and clicks, including transcribed or recorded voice queries and Google Assistant responses; browsing history, including application usage; bookmarks; passwords; autofill information; alerts, subscriptions, and other automated searches, including associated notifications and creation dates; user settings; and all associated logs and change history.

Google LLC is hereby ordered to disclose the above information to the government within 14 DAYS of service of this warrant.

II. Information to be seized by the government

All information described above in Section A that constitutes fruits, evidence, and instrumentalities of violations of Title 18, United States Code, Section 1591(a)(1) and (b)(2) (sex trafficking by force, fraud, or coercion) or Title 18, United States Code, Section 1594(b) (conspiracy to commit sex trafficking) involving Samuel L. Spencer and any co-conspirators, including:

1. Evidence related to posting of online commercial sex advertisements;

2. Images or videos of known or suspected sex trafficking victims, such as those taken for use in commercial sex advertisements or for communication with commercial sex buyers;

3. Communications with known or suspected sex trafficking victims or co-conspirators;

4. Messages, photographs, videos, memes, status updates, comments, or other postings;

5. Evidence of user attribution, showing who created or used the accounts at the time the things described in this warrant were created, edited, or deleted;

6. Evidence indicating how and when the accounts were accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the account owner(s) or user(s);

7. Evidence indicating the account owner(s) or user(s)'s state of mind as it relates to the crime under investigation; and

8. The identities of the person(s) who communicated with the accounts about matters relating to the above-listed offenses, including records that help reveal their whereabouts.